National Infrastructure Protection Center
CyberNotes

Issue #2002-12 *June 17, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between May 12 and June 13, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Aladdin Enterprises [1, 2, 3]	Unix	Ghostscript 5.50, 6.51, 6.52,	A vulnerability exists due to insufficient checking when the '.locksafe' or '.setsafe' functions are used to reset the page device, which could let a malicious user execute arbitrary commands.	**Caldera:** ftp://ftp.caldera.com/pub/updates/OpenLinux/3.1.1/Server/current/RPMS/ **RedHat:** ftp://updates.redhat.com/	Ghostscript '.locksafe' or '.setsafe' Arbitrary Command Execution CVE Name: CAN-2002-0363	High	Bug discussed in newsgroups and websites.

[1] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:083-22, June 3, 2002.
[2] Hewlett-Packard Company Security Bulletin, HPSBTL0602-047, June 5, 2002.
[3] Caldera International, Inc. Security Advisory, CSSA-2002-026.0, June 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Allaire[4]	Multiple	ColdFusion Server MX Profes-sional, Enterprise Developer	A Cross-Site Scripting vulnerability exists in the default Missing Template handler because malicious script code may be included in a missing template URI, which could let a malicious user execute arbitrary code.	Patch available at: http://download.macromedia.com/pub/security_zone/cfmx/MPSB02-03.zip	ColdFusion Missing Template Cross Site Scripting	**High**	Bug discussed in newsgroups and websites.
AnalogX[5]	Multiple	Simple Server: WWW 1.16	A remote Denial of Service vulnerability exists when a malicious user connects via Telnet and makes an invalid request to the server.	No workaround or patch available at time of publishing.	SimpleServer: WWW Web Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache Software Foundation [6]	Unix	Tomcat 3.2, 3.2.1, 3.3, 3.3.1, 4.0-4.0.3, 4.1	A Denial of Service vulnerability exists when Tomcat encounters a malicious JSP page.	No workaround or patch available at time of publishing.	Tomcat JSP Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Ayman Akt[7]	Unix	IRCIT 0.3.1	A remote Buffer Overflow vulnerability exists when a maliciously formatted INVITE message is received, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	IRCIT Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Belkin[8]	Multiple	F5D5230-4	A vulnerability exists when a forwarded request originates in the internal network and the originating IP is modified to reflect the external interface of the router, which could let a malicious user avoid detection.	No workaround or patch available at time of publishing.	F5D5230-4 Router Internal Web Request	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
BizDesign[9]	Multiple	ImageFolio 2.23, 2.24, 2.26	A vulnerability exists due to weak access control to an unprotected setup script, which could let a remote malicious user obtain administrative access.	This issue has been fixed in version 2.27 of ImageFolio Pro. Customers are advised to contact the vendor for upgrade information.	ImageFolio Unauthorized Administrative Access	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
BizDesign [10]	Multiple	ImageFolio 2.23, 2.24, 2.26, 2.27	A vulnerability exists when a category is created with a maliciously constructed name, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ImageFolio Authorized User Web Root Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[4] Macromedia Security Bulletin, MPSB02-03, June 13, 2002.
[5] Bugtraq, June 13, 2002.
[6] Vulnwatch, June 11, 2002.
[7] Gobbles Security Lab, June 12, 2002.
[8] Bugtraq, June 9, 2002.
[9] Bugtraq, June 9, 2002.
[10] Bugtraq, June 9, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Caldera[11]	Unix	OpenUnix 8.0, UnixWare 7.1.1	A vulnerability exits when the FTP server is in PASV mode because predictable PASV mode port numbers are selected, which could let a remote malicious user hijack data connections and retrieve data before the client can.	Patch available at: ftp://stage.caldera.com/pub/security/openunix/CSSA-2002-SCO.23/erg501602b.pkg.Z	Open Unix / UnixWare ftpd PASV Mode Hijacking	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Caldera International, Inc.[12]	Unix	OpenServer 5.0.5, 5.0.6	A format string vulnerability exists in the 'crontab' implementation when an error message is issued as a result of an invalid filename argument, which could let a malicious user execute arbitrary code and obtain elevate privileges.	Temporary workaround (SRT): Disable the setgid permissions.	OpenServer crontab Format String	**High**	Bug discussed in newsgroups and websites.
Caldera International, Inc[13]	Unix	Volution Manager 1.1	A vulnerability exists because the unencrypted Directory Administrator's password is stored in the /etc/ldap/slapd.conf file, which could let a malicious user obtain sensitive information.	This vulnerability will be corrected in the next release of Volution Manager. Please see advisory CSSA-2002-024.0 on how to implement the encryption feature located at: http://www.caldera.com/support/security/2002.html	Volution Manager Unencrypted Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
CGIScript.net[14]	Multiple	csNews 1.0, csNews Professional 1.0	Multiple vulnerabilities exist: a vulnerability exists because database files may be accessed by unauthorized users, which could let a malicious user obtain sensitive information; a vulnerability exists because users with "public" access to the system may be able to view and modify some administration pages when a HTTP request is submitted that contains metacharacters that are double URL encoded; and a vulnerability exists because it is possible for a malicious user to bypass file type restrictions on the header and footer file, which could let them obtain sensitive information.	No workaround or patch available at time of publishing.	csNews Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required for the database file vulnerability. Exploits have been published for the "public" access and header and footer file restrictions vulnerabilities.

[11] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.23, May 30, 2002.
[12] Strategic Reconnaissance Team Security Advisory, SRT2002-06-04-1611, June 4, 2002.
[13] Caldera International, Inc. Security Advisory, CSSA-2002-024.0, June 3, 2002.
[14] Bugtraq, June 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
CGIScript.net[15]	Unix	csPassword 1.0	Multiple vulnerabilities exist: a vulnerability exists in '.htpasswd' files because they are generated in the same folder as the '.htaccess' files, which could let a malicious user obtain usernames and passwords; a vulnerability exists in the 'csPassword.cgi' script, which could let a malicious user add directives and make changes to the generated '.htaccess file;' and a vulnerability exists in the 'csPassword.cgi' script, which could let a malicious user obtain sensitive information.	Customers are advised to contact the vendor for patch information.	csPassword Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Datalex[16]	Multiple	Bookit! Consumer 2.0	A vulnerability exists because password information is stored and passed in plain text, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.datalex.com/products_consumer24.asp	Bookit! Consumer Plaintext Password Information	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Debian[17]	Unix	Debian Linux 2.2 sparc, powerpc, Linux 2.2 IA-32, Linux 2.2 arm, alpha, Linux 2.2 68k	A vulnerability exists because 'in.uucpd' does not properly truncate strings, which could let a remote malicious user cause a Denial of Service.	Update available at: http://security.debian.org/dists/stable/updates/main/	Debian IN.UUCP Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Double Precision Incorporated[18]	Unix	Courier MTA 0.38.1	A remote Denial of Service vulnerability exists in the MTA when messages that contain an excessively large year are handled.	No workaround or patch available at time of publishing.	Courier MTA Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[15] Bugtraq, May 29, 2002.
[16] iDEFENSE Security Advisory, 06.10.2002, June 10, 2002.
[17] Debian Security Advisory, DSA-129-1, May 27, 2002.
[18] Securiteam, June 3, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Dug Song[19]	Multiple	Dsniff 2.3; Fragroute 1.2; Fragrouter 1.6	A vulnerability exists because the source code of Fragroute, Fragrouter, and Dsniff were altered to include a backdoor, which allows a remote malicious user from the IP address 216.80.99.202 to remotely execute arbitrary commands on the host that it was installed on. The source code is reported to have been corrupted on May 17, 2002. Downloads of the source from monkey.org during this time likely contain the Trojan code. A confirmed MD5 sum of a contaminated archive is: 65edbfc51f8070517f14ceeb8f721075 If a fragroute install was based on an archive with this MD5 sum, it is likely that the backdoor code was executed.	The author has stated that clean versions are available. The MD5 sums are: • MD5 (dsniff-2.3.tar.gz) = 183e336a45e38013f3af840bddec44b4 • MD5 (fragroute-1.2.tar.gz) = 7e4de763fae35a50e871bdcd1ac8e23a • MD5 (fragrouter-1.6.tar.gz) = 73fdc73f8da0b41b995420ded00533cc Note: Users are advised to install with caution.	Fragroute/ Dsniff/ Fragrouter Configure Script Trojan Horse	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
eDonkey 2000[20]	Windows	Client 35.16.59 Windows, 35.16.60 Windows	A buffer overflow vulnerability exists in the URL handler when parsing maliciously constructed URLs, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.edonkey2000.com/files/eDonkey61.exe	eDonkey 2000 Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Ehud Gavron[21]	Unix	TrACES route 6.0, 6.1, 6.1.1	A format string vulnerability exists in the terminator (-T) function due to improper use of the fprint function, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	TrACESroute Terminator Function Format String	**High**	Bug discussed in newsgroups and websites.
Eryq [22]	Unix	MIME:: Tools 5.4.11	Several vulnerabilities exist: a vulnerability exists because RFC 2231 encoding is not supported: a method of encoding MIME parameters is not supported, and the implementation used for encoding words where US-ASCII is not the default character set, which may result in a security vulnerability in software packages dependent on the module for security sensitive tasks such as e-mail content scanning.	No workaround or patch available at time of publishing.	MIME::Tools RFC Parameter Value Continuation	Medium	Bug discussed in newsgroups and websites.

[19] Bugtraq, May 31, 2002.
[20] Securiteam, June 11, 2002.
[21] DownBload Security Research Lab Advisory, June 6, 2002.
[22] Securiteam, June 5, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Evolvable Corpora-tion[23]	Windows 95/98/NT 4.0/2000	Shambala Server 4.5	Several vulnerabilities exist: a Directory Traversal vulnerability exists in the FTP server, which could let a malicious user obtain sensitive information; and a Denial of Service vulnerability exists when a malicious user sends a malformed request to the server.	No workaround or patch available at time of publishing.	Shambala Server FTP Server Directory Traversal & Denial of Service	Low/ Medium (Medium if sensitive informa-tion can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required for the Directory Traversal vulnerability. A Proof of Concept exploit has been published for the Denial of Service.
Geeklog[24]	Multiple	Geeklog 1.3.5	Multiple vulnerabilities exist: a vulnerability exists because externally-supplied input that is used in SQL queries is not properly validated, which could let a malicious user execute arbitrary SQL commands; multiple Cross-Site Scripting vulnerabilities exists because script code is not properly filtered from URL parameters, which could let a malicious user execute arbitrary script code; and a vulnerability exists because script code is not properly sanitized from form fields, which could let a malicious user execute arbitrary script code.	Patch available at: http://prdownloads.sourceforge.net/geeklog/geeklog-1.3.5sr1.tar.gz	Geeklog Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
Hewlett Packard, Systems[25]	Unix	HP-UX 11.0, 11.11	A Denial of Service vulnerability exists in the HP-UX Software Distributor (SD) because a data view of files not normally readable by a user is allowed.	Patches available at: http://itrc.hp.com PHCO_25875 PHCO_25887	HP-UX SD Data View Denial Of Service	Low	Bug discussed in newsgroups and websites.
IBM[26]	Unix	Informix SE 7.25.UC1	A buffer overflow vulnerability exists if the 'INFORMIXDIR' environment variable is defined with a size greater than 2023 bytes, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	Informix SE Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[23] Telhack 026 Inc. Security Advisory #3, May 30, 2002.
[24] ALPER Research Labs Security Advisory, ARL02-A13, June 10, 2002.
[25] Hewlett-Packard Company Security Bulletin, HPSBUX0205-194, May 30, 2002.
[26] Bugtraq, May 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ikonboard.com[27]	Multiple	Ikonboard 3.0 .1	A vulnerability exists because Flash content may be uploaded, which could let a malicious user execute arbitrary JavaScript.	No workaround or patch available at time of publishing.	Ikonboard Flash File	**High**	Bug discussed in newsgroups and websites.
Internet Security Systems[28]	Windows 95/98/ME/ NT 4.0/2000, XP	BlackIce Agent 3.1 EAL	A vulnerability exists in the default installation because the Agent might not reactivate when the host returns from standby, which could let a malicious user bypass the firewall completely.	Upgrade available at: https://bvlive01.iss.net/issEn/DLC/login.jhtml	BlackIce Firewall Bypass	Medium	Bug discussed in newsgroups and websites.
ISC[29, 30, 31, 32, 33,]	Unix	BIND 9.0, 9.1-9.1.3, 9.2	A remote Denial of Service vulnerability exists when a malicious user sends a specific DNS packet that is designed to trigger an internal consistency check. *Note: Because the normal operation of most services on the Internet depends on the proper operation of DNS servers, other services could be affected if this vulnerability is exploited.*	**ISC:** ftp://ftp.isc.org/isc/bind9/9.2.1/bind-9.2.1.tar.gz **RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **SuSE:** ftp://ftp.suse.com/pub/suse/ **Caldera:** ftp://ftp.caldera.com/pub/updates/OpenUNIX/	ISC BIND 9 Remote Denial Of Service CVE Name: CAN-2002-0400	Low/**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Jon Hedley[34]	Multiple	AlienForm 2 1.5	A Directory Traversal vulnerability exists when a file path is constructed with special characters, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	AlienForm2 Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
LBL[35, 36, 37, 38, 39, 40]	Unix	tcpdump 3.6.2	A remote buffer overflow vulnerability exists when malformed NFS packets are handled, which may let a remote malicious user execute arbitrary instructions with the privileges of the tcpdump process.	**Conectiva:** ftp://atualizacoes.conectiva.com.br/ **RedHat:** ftp://updates.redhat.com/ **Caldera:** ftp://ftp.caldera.com/pub/updates/OpenLinux/ **SuSE:** ftp://ftp.suse.com/pub/suse/ **Mandrake Linux:** http://www.mandrakesecure.net/en/ftp.php	TCPDump Malformed NFS Packet Buffer Overflow CVE Name: CAN-2002-0380	**High**	Bug discussed in newsgroups and websites.

[27] EyeonSecurity, June 5, 2002.
[28] KPMG-2002019, June 6, 2002.
[29] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:105-09, June 4, 2002.
[30] Hewlett-Packard Company Security Bulletin, HPSBTL0206-045, June 5, 2002.
[31] Conectiva Linux Security Announcement, CLA-2002:494, June 6, 2002.
[32] SuSE Security Announcement, SuSE-SA:2002:021, June 6, 2002.
[33] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.24, June 10, 2002.
[34] Bugtraq, June 10, 2002.
[35] Conectiva Linux Security Announcement, CLA-2002:491, June 6, 2002.
[36] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:094-08, May 29, 2002.
[37] Caldera International, Inc. Security Advisory, CSSA-2002-025.0, June 4, 2002.
[38] SuSE Security Announcement, SuSE-SA:2002:020, May 29, 2002.
[39] Mandrake Linux Security Update Advisory, MDKSA-2002:032, May 16, 2002.
[40] Hewlett-Packard Company Security Advisory, HPSBTL0205-044, June 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Linksys[41]	Multiple	EtherFast BEFSR11 Router 1.42.7, BEFSR41 Router 1.42.7, BEFSRU31 Router 1.42.7	A vulnerability exists in the current firmware because existing rules that deny remote administration of the router are not respected, which could allow remote administration by a malicious user even if it has been specifically disabled in the product	No workaround or patch available at time of publishing.	EtherFast Router Remote Administration Enabled	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
LogiSense Corporation[42]	Multiple	DNS Manager System, Hawk-i 5.2, Hawk-i ASP	A vulnerability exists in the ASP based login process because user input is not adequately filtered, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Hawk-i ASP Login	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Lokwa[43]	Multiple	Lokwa BB 1.2.1	A vulnerability exists because externally-supplied input is not properly validated when arbitrary characters and additional SQL statements are included in a query, which could let a malicious user obtain sensitive information	No workaround or patch available at time of publishing.	Lokwa BB Sensitive Information	Medium	Bug discussed in newsgroups and websites.
Luis Bernardo[44]	Multiple	MyHelp Desk 20020509	Multiple vulnerabilities exist: a vulnerability exists because HTML tags are not properly sanitized from form fields, which could let a malicious user execute arbitrary HTML script code; multiple Cross-Site Scripting vulnerabilities exist due to unsanitized CGI parameters, which could let a malicious user execute arbitrary script code; and a SQL injection vulnerability exists because user input is not properly sanitized, which could let a remote malicious user modify the logic of a SQL query.	No workaround or patch available at time of publishing.	MyHelpDesk Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Macro-media[45]	Multiple	JRun 3.0, 3.1, 4.0	A Denial of Service vulnerability exists when JRun encounters a malicious JSP page.	No workaround or patch available at time of publishing.	JRun JSP Page Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[41] Securiteam, June 9, 2002.
[42] Bugtraq, June 4, 2002.
[43] SecurityFocus, June 10, 2002.
[44] ALPER Research Labs Security Advisory, ARL02-A15, June 10, 2002.
[45] Vulnwatch, June 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Marc Druilhe[46]	Multiple	W-Agora 4.1.1-4.1.3	A vulnerability exists in the 'inc_dir' variable in several scripts, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	W-Agora Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Matsushita Research[47]	Unix	MNews 1.2.2	Multiple local and remote buffer overflow vulnerabilities exist due to improper bounds checking on certain command line arguments as well as the MAILSERVER and JNAMES environment variables, which could let a local malicious user obtain elevated privileges and a remote malicious user use MNews to penetrate an affected system.	No workaround or patch available at time of publishing.	MNews Multiple Buffer Overflows	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Matthew Mondor[48]	Unix	mmftpd .7	A format string vulnerability exists in the mmftpd FTP deamon due to improper use of the syslog call, which could let remote malicious user execute arbitrary code.	Upgrade available at: http://mmondor.gobot.ca/software/linux/mmftpd-0.0.8.tar.gz	MMFTPD SysLog Format String	**High**	Bug discussed in newsgroups and websites.
Matthew Mondor[49]	Unix	mmmail .11, .12, .13	A vulnerability exists due to improper use of the syslog call, which could let a malicious user execute arbitrary code.	Update available at: http://mmondor.gobot.ca/software/linux/mmmail-0.0.14.tar.gz	MMMail Remote SysLog Format String	**High**	Bug discussed in newsgroups and websites.
Microsoft[50]	Windows	.NET Framework 1.0 SP1, 1.0	A buffer overflow vulnerability exists because a function that processes cookie data in the ASPState service fails to properly check the length of the cookies passed to it, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-026.asp *Note: Microsoft encourages users not to install the patch while VS.NET is running.*	Microsoft ASP.NET StateServer Buffer Overflow CVE Name: CAN-2002-0369	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Microsoft[51]	Windows NT 4.0/2000	IIS 4.0, 5.0	A buffer overflow vulnerability exists because of an arithmetic error in the ISAPI extension that implements the HTR functionality, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-028.asp	Microsoft IIS ISAPI Extension Buffer Overflow CVE Name: CAN-2002-0364	**High**	Bug discussed in newsgroups and websites.

[46] SecurityFocus, June 10, 2002.
[47] Strategic Reconnaissance Team Security Advisory, SRT2002-04-31-1159, May 31, 2002.
[48] INTEXXIA(c) Security Advisory, #1053-040602, June 6, 2002.
[49] INTEXXIA(c) Security Advisory, #1054-040602, June 12, 2002.
[50] Microsoft Security Bulletin, MS02-026 Ver 2.0, June 7, 2002.
[51] Microsoft Security Bulletin, MS02-028, June 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[52]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0; Proxy Server 2.0; ISA Server 2000	A buffer overflow vulnerability exists in the component that parses gopher replies, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-027.asp	Multiple Microsoft Product Gopher Client Buffer Overflows CVE Name: CAN-2002-0371	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[53]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.5, 5.5 SP1&2. 6.0	A Cross-Site Scripting vulnerability exists if both the "Enable folder view for FTP sites" and the "Enable Web content in folders" options are enabled, which could let a malicious user execute arbitrary JavaScript code.	No workaround or patch available at time of publishing.	Internet Explorer Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[54] ***Microsoft updates bulletin***[55]	**Multiple**	**MSN Chat Control**	**A buffer overflow vulnerability exists in the ActiveX control, which could let a remote malicious user execute arbitrary code on the system with the privileges of the current user.** ***Bulletin updated to advise customers that the fixes released on May 08, 2002 did not fully protect systems against the reintroduction of the older, vulnerable control and to announce the availability of updated fixes.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-022.asp** ***Updates fixes available at:*** http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-022.asp	**MSN Chat Control Remote Buffer Overflow** **CVE Name: CAN-2002-0155**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**
Microsoft[56]	Windows NT 4.0/2000	SQL Server 2000, 2000 SP1&2	Two vulnerabilities exist: a buffer overflow vulnerability exists in the SQLXML ISAPI extension that handles data queries over HTTP(SQLXML HTTP) when malformed data is received, which could let a malicious user execute arbitrary code; and a vulnerability exists because it is possible to inject arbitrary script code via XML tags, which could let a malicious user execute arbitrary script code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-030.asp	Microsoft SQL Server Vulnerabilities CVE Name: CAN-2002-0186, CAN-2002-0187	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.

[52] Microsoft Security Bulletin, MS02-027 V2.0, June 14, 2002.
[53] Bugtraq, June 7, 2002.
[54] Microsoft Security Bulletin, MS02-022, May 8, 2002.
[55] Microsoft Security Bulletin, MS02-022 V2.0, June 11, 2002.
[56] Microsoft Security Bulletin, MS02-030, June 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[57]	Windows NT 4.0/2000, XP	Visual Basic .NET, Visual C# .NET, Visual C++.Net, Visual Studio .NET Academic Edition, Enterprise Architect Edition, Enterprise Developer Edition, Profes-sional Edition, Trial Edition	Microsoft has discovered that the Nimda virus has been detected in one of the Help files that are included in the Korean language version of Microsoft Application Center Test (ACT). Installing or using the Korean version of Microsoft Visual Studio .NET does not cause an infection. A user with sufficient privileges that executes this file could potentially infect the host with Nimda. This may result in the host becoming susceptible to the problems associated with the W32/Nimda malicious code. While this the infection is believed to be inert, there is some possibility that the worm could be triggered.	For the English-language instructions about how to download and install the Korean version of the Visual Studio .NET update, visit the following Microsoft Web site: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=39788 For the Korean-language instructions about how to download and install the Korean version of the Visual Studio .NET update, visit the following Microsoft Web site: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=39262	Visual Studio .NET Korean Version Nimda Infected	Medium	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.

[57] Microsoft, June 13, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[58]	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Profes-sional, 2000 Profes-sional SP1&2, 2000 Server, 2000 Server SP1&2, NT Enterprise Server 4.0, NT Enterprise Server 4.0 SP1-6a, NT Server 4.0, NT Server 4.0 SP1-61a, NT Terminal Server 4.0, NT Terminal Server 4.0 SP1-6a, NT Work-station 4.0, NT Work-station 4.0 SP1-6a, XP 64-bit Edition, XP Home, XP Profes-sional	A buffer overflow vulnerability exists in the Remote Access Server (RAS) Phonebook service when a specially malformed phonebook entry is sent, which could let a malicious user obtain elevated privileges, and gain complete control over the machine.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-029.asp	Windows 2000 Remote Access Service Buffer Overflow CVE Name: CAN-2002-0366	**High**	Bug discussed in newsgroups and websites.

[58] Microsoft Security Bulletin, MS02-029, June 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla[59]	Multiple	Bugzilla 2.14, 2.14.1	Several vulnerabilities exist which could let a remote malicious user obtain sensitive information. A vulnerability exists in the 'queryhelp.cgi' script because it does not observe any restrictions that may be set on the display of products in the Bugzilla database; it is possible for a malicious user to bypass the IP check by setting up a fake reverse DNS, if the Bugzilla web server was configured to do reverse DNS lookups; a vulnerability exists because in some situations the data directory became world writeable; a vulnerability exists because a malicious user with access to 'editusers.cgi' could delete a user regardless of whether 'allowuserdeletion' is on; a Cross-Site Scripting vulnerability exists because real names are not HTML filtered; a vulnerability exits because a mass change will set the groupset of every bug to be the same groupset of the first bug; a vulnerability exits because Bugzilla does not handle encoding from some browsers which could lead to unexpected consequences; and a vulnerability exists because it is possible for random confidential information to be divulged, if the shadow database is in use and becomes corrupted.	Upgrade available at: http://ftp.mozilla.org/pub/webtools/bugzilla-2.14.2.tar.gz	Multiple Bugzilla Security	Medium	Bug discussed in newsgroups and websites. Many of these vulnerabilities can be exploited via a web browser.

[59] Bugzilla Security Advisory, June 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla/ Netscape[60]	Windows 95/98/ME/ NT 4.0/2000, XP, Mac OS 9.0, 9.0.4, 9.1, 9.2, MacOS X 10.x, Unix	Mozilla Browser 0.9.2.1, 0.9.2, 0.9.3, 0.9.4.1, 0.9.4-0.9.9, 1.0, 1.0 RC1&2; Netscape Communi-cator 4.0.4-4.08, 4.0, 4.5-4.7, 4.51, 4.61, 4.72-4.77, Netscape 6.0 1, 6.0 Mac, 6.0-6.2.2	A Denial of Service vulnerability exists when malformed e-mail messages are received, which could prevent clients from accessing POP3 mailboxes.	This issue is resolved in Mozilla 1.1. Alpha versions may be accessed at: http://www.mozilla.org/releases/	Netscape / Mozilla Malformed E-mail Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape[61]	Windows 95/98/NT 4.0/2000, Unix	Communi-cator 4.77	A buffer overflow vulnerability exists in the Composer function when an HTML page is edited that contains a Font Face field of arbitrary length, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Netscape Composer Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
NetScreen [62]	Multiple	ScreenOS 3.0.3 r1.1	A vulnerability exists because HTML tags are not filtered from authentication fields, which could let a malicious user cause the log files to appear as though they have been deleted.	No workaround or patch available at time of publishing.	ScreenOS HTML File Display	Medium	Bug discussed in newsgroups and websites.
Novell[63]	Multiple	eDirectory 8.6.2, 8.7	A vulnerability exists because case-insensitive passwords are allowed, which decreases the number of unique passwords. As a result, a brute-force attack may be more feasible.	No workaround or patch available at time of publishing.	eDirectory Weak Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Nullsoft[64]	Unix	Shoutcast Server 1.8.9 Win32, Solaris, Mac OS X, Linux, FreeBSD	A buffer overflow vulnerability exists, which could let a remote malicious unauthorized user execute arbitrary code.	No workaround or patch available at time of publishing.	Shoutcast Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[60] Bugtraq, May 12, 2002.
[61] Infobyte Security Research, June 13, 2002.
[62] SecurityFocus, June 5, 2002.
[63] Bugtraq, May 30, 2002.
[64] Netric Security Team, June 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Patrick Powell[65]	Unix	LPRng 3.7.4, 3.8.9	A vulnerability exists because default configurations of LPRng accept all remote print submissions to the print queue, which could let a malicious user submit numerous print requests to the existing print queue.	Update available at: ftp://updates.redhat.com/7.0/en/os/	LPRNG Remote Print Submission CVE Name: CAN-2002-0378	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
PHP-Reactor[66]	Multiple	Ekilat LLC php(Reactor) 1.2.7	A Cross-Site Scripting vulnerability exists in the 'browse.php,' in the "comments" section because user input is not properly filtered, which could let a remote malicious user execute arbitrary script code.	Upgrade available at: http://prdownloads.sourceforge.net/phpreactor/phpreactor-1.2.7pl1.tar.gz?download	Global.INC. PHP Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
QNX Software Systems Ltd.[67]	Multiple	QNX RTOS 4.25, 6.1.0	Multiple vulnerabilities exist: a vulnerability exists in the 'su' utility which could let a malicious user obtain sensitive information; a vulnerability exists in the 'phgrafx' utility, which could let a malicious user obtain elevated privileges and root access; a vulnerability exists in the 'phgrafx-startup' utility, which could let a malicious user obtain elevated privileges and root access; a buffer overflow vulnerability exists in the 'phlocale' utility, which could let a malicious user execute arbitrary code as root; and a vulnerability exists in the ptrace() implementation, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	QNX RTOS Multiple Vulnerabilities	Medium/ **High** **(High if root access can be obtained or arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of concept exploit has been published. Exploit scripts for the 'phgrafx,' 'phgrafx-startup,' and 'phlocale' utilities and the ptrace() implementation vulnerabilities have been published.
QNX Software Systems Ltd.[68]	Multiple	RTOS 6.1.0	A buffer overflow vulnerability exists in the 'pkg-installer' utility, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	QNX RTOS PKG-Installer Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[65] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:089-07, June 9, 2002.
[66] ALPER Research Labs Security Advisory, ARL02-A12, June 6, 2002.
[67] Bugtraq, June 3, 2002.
[68] Bugtraq, June 3, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
QNX Software Systems, Ltd.[69]	Multiple	RTOS 4.25	Multiple vulnerabilities exist: a vulnerability exists in the 'crttrap' binary, which could let a malicious user obtain sensitive information; a vulnerability exists in the monitor –f command line option, which could let a malicious user modify arbitrary system files; a vulnerability exists in the Watcom sample utility, which could let a malicious user overwrite root-owned, read-only files and possibly obtain root access; a vulnerability exists in the 'dumper' debugging utility when memory dump files are created because it follows symbolic links, which could let a malicious user overwrite and gain ownership of arbitrary files and elevate to root privileges; a buffer overflow vulnerability exists in the 'sample' utility, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'int10' utility when excessively long filename parameters are argumented, which may let a malicious user obtain root privileges.	Upgrade available for the monitor utility and dumper debugger utility vulnerabilities at: http://get.qnx.com No workaround or patch available at time of publishing for other vulnerabilities.	QNX RTOS Multiple Vulnerabilities	Medium/ **High** **(High if root access can be obtained)**	Bug discussed in newsgroups and websites. Exploits have been published.
Quantum[70]	Multiple	Snap Server 4100	Several vulnerabilities exist: a vulnerability exists because the TCP/IP protocol stack uses predictable sequence numbers, which could let a malicious user hijack existing connections; and a Denial of Service vulnerability exists when the Snap Server is portscanned.	No workaround or patch available at time of publishing.	Snap Server TCP Sequence Number and Denial of Service	Low/ Medium (Medium if an existing connec-tion can be hijacked)	Bug discussed in newsgroups and websites. There is no exploit code required.
RedHat[71]	Unix	RHMask 1.0 -9	A vulnerability exists because the output filename supplied in mask files is not properly validated, which could let a malicious user overwrite arbitrary system files.	No workaround or patch available at time of publishing.	RHMask Local File Overwrite	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[69] Bugtraq, May 31, 2002.
[70] Bugtraq, May 30, 2002.
[71] Bugtraq, June 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Red-M Communi-cations Ltd.[72]	Multiple	1050AP LAN access point	Multiple vulnerabilities exist: a Denial of Service vulnerability exists in the 1050AP device because the system has no concept of authorized or unauthorized hosts and is simply protected by a password over an unencrypted connection; a Denial of Service vulnerability exists in the AP because the administration password is not case sensitive; a Denial of Service vulnerability exists when an unusually long string of data is supplied in the PPP username field; a vulnerability exists in the tftp server for configuration backups and firmware updates because it can not be disabled and can be used by a malicious user to crack the administration password using a UDP based attack; and a vulnerability exists within the administration web interface, which could let a malicious user obtain unauthorized access.	Denial of service vulnerabilities upgrade available at: http://www.red-m.com/Products/Downloads/freefiles/1050AP_2_02_10.zip No workaround or patch available at time of publishing for other vulnerabilities.	Multiple Red-M 1050 Blue Tooth Access Point Vulnerabilities CVE Names: CAN-2002-0393, CAN-2002-0394, CAN-2002-0395, CAN-2002-0396, CAN-2002-0397, CAN-2002-0398	Low/ Medium (Medium if unauth-orized access can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
Richard Gooch[73]	Unix	simpleinit 2.0.2	A vulnerability exists because some child processes are allowed to inherit a file descriptor with read-write access, which could let a malicious user execute arbitrary commands as the superuser.	No workaround or patch available at time of publishing.	SimpleInit Inherit File Descriptor	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Ruslan Communic ations[74]	Multiple	<Body> Builder	A vulnerability exists because user supplied input for the login password is not properly filtered, which could let a malicious user obtain unauthorized administrative access.	No workaround or patch available at time of publishing.	Ruslan Communi-cations <Body>Builder SQL Injection	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
SCO[75]	Unix	Open Server 5.0-5.0.6	A vulnerability exists in XSCO when an excessively long argument is supplied to the 'co' flag, which could let a malicious user execute arbitrary code with elevated privileges.	No workaround or patch available at time of publishing.	OpenServer XSCO Heap Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[72] @stake Inc. Security Advisory, June 5, 2002.
[73] SecurityFocus, June 12, 2002.
[74] Bugtraq, June 13, 2002.
[75] Strategic Reconnaissance Team Security Advisory, SRT2002-06-11-1037, June 10, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Scripts For Educators[76]	Multiple	MakeBook 2.2	A vulnerability exists because form field input is not properly sanitized, which could let a remote malicious user execute arbitrary HTML.	No workaround or patch available at time of publishing.	MakeBook Input Validation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Seanox[77]	Windows	DevWex Windows Binary 1.2002.0520	Several vulnerabilities exist: a Directory Traversal vulnerability exists because certain sequences from web requests are not sufficiently filtered, which could let a malicious user obtain sensitive information; and a buffer overflow vulnerability exits in the GET request function, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.seanox.de/projects.devwex.php4	DevWex Multiple Vulnerabilities	Low/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerabilities can be exploited via a web browser.
SGI[78]	Unix	IRIX 5.0-5.3, 6.0-6.5.16	A vulnerability exists in MediaMail when certain command line arguments are passed to it, which could let a malicious user obtain sensitive information and elevated privileges.	MediaMail is an expired product, therefore SGI has not provided patches for these vulnerabilities. SGI recommends uninstalling the program and switching to a different mail program.	IRIX MediaMail Memory Corruption CVE Name: CAN-2002-0358	Medium	Bug discussed in newsgroups and websites.
SGI[79]	Unix	IRIX 6.5-6.5.15, 6.5.2f-6.5.15f, 6.5.2m-6.5.15m	A buffer overflow vulnerability exists in the NIS password server, 'rpc.passwd', which could let a remote malicious user obtain root access.	Patch available at: http://support.sgi.com/irix/swupdates/	IRIX rpc.passwd Buffer Overflow CVE Name: CAN-2002-0357	**High**	Bug discussed in newsgroups and websites.
Splatt.it[80]	Multiple	Splatt Forum 3.0	A vulnerability exists because HTML is not filtered from image tags, which could let a malicious user execute arbitrary script code.	Upgrade available at: www.splatt.it	Splatt Forum Image Tag HTML Injection	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Stellar-X Software[81]	Windows NT	MSNTAuth 2.0	A vulnerability exists when data is passed to the syslog() as the format string argument, which may let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Stellar-X Format String	**High**	Bug discussed in newsgroups and websites.

[76] DownBload Security Research Lab Advisory, June 12, 2002.
[77] Securiteam, June 11, 2002.
[78] SGI Security Advisory, 20020602-01-I, June 6, 2002.
[79] SGI Security Advisory, 20020601-01-P, June 4, 2002.
[80] Bugtraq, June 6, 2002.
[81] David Evlis Reign Security Advisory #11, June 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Stephen Hebditch[82]	Unix	slurp 1.10	A format string vulnerability exists in the syslog function, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Slurp Remote Format String	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Sun Micro-Systems, Inc.[83]	Unix	Sun Solaris 2.6 _x86, 2.6, 7.0 _x86, 7.0, 8.0 _x86, 8.0	Two vulnerabilities exist: a format string vulnerability exists in the 'snmpdx' component, which could let a remote malicious user execute arbitrary code with root privileges; and a buffer overflow vulnerability exists in 'mibiisa' due to an unsafe memory copy operation, which could let a malicious user overwrite the return address with an arbitrary value.	Patch available at: http://sunsolve.sun.com/securitypatch	Sun Solaris snmpdx Format String & mibiisa Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Teekai[84]	Multiple	Forum 1.2	Several vulnerabilities exist: a vulnerability exists because user cookies are stored in a non-encrypted format, which could let a malicious user obtain unauthorized access including the administrative account; and a vulnerability exists due to weak encryption of web usage statistics, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Forum Multiple Vulnerabilities	Medium/ **High** **(High if adminis-trative access can be obtained)**	Bug discussed in newsgroups and websites. Exploit has been published for the web statistics weak encryption vulnerability.
Teekai[85]	Multiple	Tracking Online 1.0	A Cross-Site Scripting vulnerability exists because HTML tags are not adequately filtered from certain URL parameters, which could let a malicious user create an arbitrary link to a vulnerable webpage.	No workaround or patch available at time of publishing.	Tracking Online Cross-Site Scripting	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Telindus[86]	Multiple	1110 ADSL Router , 1120 ADSL Router	A vulnerability exists because the password is sent in plain text when connecting to the router via the administrative software, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	1100 Series Router Administration Password Leak	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[82] Strategic Reconnaissance Team Security Advisory, SRT2002-06-04-1011, June 4, 2002.
[83] Sun Microsystems, Inc. Security Bulletin, #00219, June 4, 2002.
[84] SecurityFocus, June 3, 2002.
[85] SecurityFocus, June 3, 2002.
[86] Bugtraq, June 5, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
The XMB Group[87]	Multiple	XMB Forum 1.6 Magic Lantern	A Cross-Site Scripting vulnerability exists because script code is not properly filtered from URL parameters, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	XMB Forum Magic Lantern Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Transware [88]	Multiple	Active! Mail 1.422, Mail 2.0	A vulnerability exists because e-mail headers are not properly stripped of HTML code prior to display, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.transware.co.jp/active/download/am_download.html	Active Mail HTML Injection	**High**	Bug discussed in newsgroups and websites.
University of Washing-ton[89]	Unix	Pine 4.21, 4.30, 4.33, 4.44	A vulnerability exists because user names and/or ids can still be leaked due to Pine's insertion of "Sender:" and/or "X-Sender:" headers, which could let a remote malicious use obtain sensitive information.	No workaround or patch available at time of publishing.	Pine Unix Sensitive Information	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Voxel Dot Net[90]	Multiple	CBMS 0.7	Multiple Cross-Site Scripting and SQL injection vulnerabilities exist, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	CBMS Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Washing-ton University [91]	Multiple	wu-imapd 2001.0a	A vulnerability exists in configurations where users are not authorized shell access to a system, but have a valid account from which to download mail via IMAP, which could let a malicious user obtain sensitive information.	The University of Washington IMAP FAQ gives information to secure affected servers located at: http://www.washington.edu/imap/IMAP-FAQs/index.html#5.1	IMAP Arbitrary File Access	Medium	Bug discussed in newsgroups and websites.
Working Resources Inc.[92]	Windows 95/98/ME/ NT 4.0/2000, XP	BadBlue 1.7 .0	A vulnerability exists if a remote malicious user appends the unicode variant of the "%" symbol, which could let a remote malicious user obtain sensitive information.	Upgrade available at: Windows 95/NT http://www.badblue.com/bb95.exe Windows 98/ME/200, XP http://www.badblue.com/bb98.exe	BadBlue Directory Contents Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
XFree86[93]	Unix	X11R6 4.0, 4.0.1, 4.0.2–11, 4.0.3, 4.1.0, 4.1-12, 4.1-11, 4.2.0	A remote Denial of Service vulnerability exists when a malicious user passes an overly large font size to the X Window system.	No workaround or patch available at time of publishing.	X Window System Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[87] Security Bugware, June 5, 2002.
[88] SNS Advisory No.54, June 13, 2002.
[89] Bugtraq, June 7, 2002.
[90] Bugtraq, June 6, 2002.
[91] Bugtraq, June 1, 2002.
[92] Bugtraq, June 1, 2002.
[93] Bugtraq, June 10, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
YaBB[94]	Windows 95/98/NT 4.0/2000	YaBB 1 Gold Release	A vulnerability exists because Flash content may be uploaded, which could let a malicious user execute arbitrary JavaScript.	No workaround or patch available at time of publishing.	YaBB Flash File Script Injection	**High**	Bug discussed in newsgroups and websites.
ZenTrack[95]	Multiple	ZenTrack 2.0.1 c Beta, 2.0.2 c Beta, 2.0.3	A path disclosure vulnerability exists if a maliciously crafted HTTP request is submitted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ZenTrack Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between May 12 and June 12, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 27 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
June 12, 2002	**GOBBLES-invite.c**	**Script which exploits the IRCIT Remote Buffer Overflow vulnerability.**
June 12, 2002	Hydra-2.1.tar.gz	A parallized login hacker which understands FTP, POP3, IMAP, Telnet, HTTP Auth, NNTP, VNC, ICQ, Socks5, PCNFS, samba, Crisco enable, LDAP, and more.
June 12, 2002	**Simpleinitexploit.c**	**Script which exploits the SimpleInit Inherit File Descriptor vulnerability.**

[94] EyeonSecurity, June 5, 2002.
[95] ALPER Research Labs Security Advisory, ARL02-A14, June 10, 2002.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
June 10, 2002	Voodoo2.tar.gz	A library which makes heap overflow exploitation much easier by providing the user with valuable internal data from Doug Lea's malloc implementation.
June 9, 2002	Ciscokill.c	Script that exploits Cisco 2600 routers spoofed snmpv1 get request vulnerability.
June 5, 2002	Bed-0.2.zip	A Perl script that remotely detects unknown buffer overflow vulnerabilities in FTP, SMTP, and POP daemons.
June 4, 2002	**Mayday-linux.c**	**Script which exploits the SHOUTCast Remote Buffer Overflow vulnerability.**
June 4, 2002	Tcc.tar.gz	TCP Congestion paper and proof of concept code for a vulnerability in the TCP protocol that affects several OS's, allowing remote denial of service attacks.
June 3, 2002	Airsnort-0.2.1.tar.gz	A tool for wireless LANs which recovers encryption keys by passively monitoring transmissions, and computing the encryption key when enough packets have been gathered. Works on both 40 and 128 bit encryption.
June 3, 2002	Dnshijacker.tar.gz	A libnet/libpcap based packet sniffer & dns spoofer tool that supports tcpdump style filters that allow you to specifically target victims.
June 3, 2002	Ettercap-0.6.6.6.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
June 3, 2002	**Mnews-1.22.pl**	**Perl script which exploits the MNews Remote FreeBSD Buffer Overflow vulnerability.**
June 3, 2002	Nessus-1.2.1.tar.gz	An up-to-date, and full featured remote security scanner for Linux, BSD, Solaris and some other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over 900 remote security checks.
June 3, 2002	**Phgrafx.sh**	**Exploit for the QNX RTOS Multiple Vulnerabilities.**
June 3, 2002	**Phgrafx-startup.sh**	**Exploit for the QNX RTOS Multiple Vulnerabilities.**
June 3, 2002	**Phlocale.c**	**Script which exploits the QNX RTOS Multiple Vulnerabilities.**
June 3, 2002	**Pkg-installer.c**	**Script which exploits the QNX RTOS PKG-Installer Buffer Overflow vulnerability.**
June 3, 2002	**Qnx-gdb-root.sh**	**Exploit for the QNX RTOS Multiple Vulnerabilities.**
June 3, 2002	Servletexeccrash.c	Script which exploits the NewAtlanta ServletExec ISAPI 4.1 Remote Denial of Service vulnerability.
June 2, 2002	**D7-ibm-x.c**	**Script which exploits the Informix SE Buffer Overflow vulnerability.**
June 2, 2002	Elfsh-0.43a.tgz	An automated reverse engineering tool for the ELF format that has a sophisticated output with cross references using .got, .ctors, .dtors, .symtab, .dynsym, .dynamic, .rel.* and many other with an integrated hexdump.
June 2, 2002	Libfmtb-0.3.tgz	A library that contains lots of functions for easily exploiting local and remote format string vulnerabilities.
June 2, 2002	Mimedefang-2.14.tar.gz	A flexible MIME e-mail scanner designed to protect Windows clients from viruses and other harmful executables.
June 2, 2002	Ymxp.txt	Exploit for the Yahoo! Messenger Buffer Overflow vulnerability for Windows XP Pro
May 30, 2002	**Ibm-sqlexec.c**	**Script which exploits the Informix SE Buffer Overflow vulnerability.**
May 30, 2002	**Ibm-sqlexec.pl**	**Script which exploits the Informix SE Buffer Overflow vulnerability.**
May 12, 2002	Eldre8.c	Script which exploits the Mozilla Malformed E-mail Denial of Service vulnerability.

Trends

- **The CERT Coordination Center (CERT/CC) has issued an advisory on a new vulnerability in the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND). The vulnerability is in version 9 to 9.2 and not in versions 4 or 8. Exploitation of this vulnerability will cause vulnerable BIND server(s) to abort and shut down. For more information, see "Bugs, Holes, & Patches" table and NIPC Advisory 02-004.1, located at: http://www.nipc.gov/warnings/advisories/2002/02-004.htm.**
- **The National Infrastructure Protection Center (NIPC) is monitoring an Internet worm called "Spida," also known as SQLSnake. This worm takes advantage of default settings within Microsoft's SQL Server (MSSQL) when there is a system administrator username of "sa" and no password. Administrators are advised to change all passwords on infected machines, not simply that of the system administrator account, For more information see NIPC Advisory 02-003 located at: http://www.nipc.gov/warnings/advisories/2002/02-003.htm.**
- There has been an increase in the number of scans to port 80 scans, still being caused by Nimda and Code Red.
- There has been an increase in the number of scans to port 1433 lately. The most common use of this port is Microsoft's SQL server. A vulnerability in SQL Server 7.0 and 2000 exists which allows access to the security context of the server. Microsoft released an advisory and a patch for this problem which is available at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-020.asp.

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Bat/Cup-A (Batch File Worm): This worm arrives in an e-mail message with the characteristics:

- Subject line: "WorldCup News!"
- Message text: "read me for more world cup news!"
- Attached file: WorldCup.BAT.

When executed, the worm will create, execute, and on occasions delete the files worldcup_score.vbs, eyeball.reg, japan.vbs, england.vbs, ireland.vbs, uraguay.vbs and argentina.bat. Worldcup_score.vbs is the file that executes the mass mailing properties of the worm. An e-mail with the above characteristics will be sent to all contacts in the user's Microsoft Outlook address book. Eyeball.reg creates the registry value:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\cqlyg

so that a copy of the worm is run when Windows starts up. An attempt will be made to copy eyeball.reg over all REG files contained in folders in the user's path and the Windows current and parent folders. Japan.vbs will attempt to start a copy of the worm called argentina.bat. An attempt will be made to copy japan.vbs over all VBS files contained in the folders of the users path and the Windows, current and parent folders. England.vbs will set the registry value:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\eifxi

so that a copy of the worm is run when Windows starts up. Ireland.vbs attempts to create a shortcut in the root folder to a copy of the worm. The shortcut would be called pif.lnk. Uraguay.vbs attempts to create a shortcut to brazil.vbs that in turn will try to execute paraguay.vbs. Paraguay.vbs does not exist. The worm creates copies of itself using the names world_cup_.bat, germany.bat, china.bat, russia.bat, turkey.bat, denmark.bat, costarica.bat, wini.bat, spain.bat, and italy.bat. These copies are most likely to be in the Windows folder. The following anti-virus related executables will be deleted:

- C:\progra~1\norton~1*.exe

- C:\progra~1\kasper~1\avp32.exe
- C:\progra~1\trojan~1\tc.exe
- C:\progra\norton~1\s32integ.dll
- C:\progra\f-prot95\fpwm32.dll
- C:\progra\tbav\tbav.dat
- C:\progra \mcafee\scan.dat
- C:\progra\avpersonal\antivir.vdf
- C:\tbavw95\tbscan.sig

Bat/Cup-A searches for a mIRC installation and creates the file script.ini if one is found. The script.ini file will attempt to forward a copy of the worm to anyone who joins an IRC channel the infected user is currently logged on to. The folder C:\ThisIsOnlyASimpleWorm will be created and will contain a single copy of the worm named WorldCup.bat. This worm contains many bugs and several of the above characteristics are intended functions of the worm and may not work correctly.

HTML_HAIYASP.A (HTML Virus): This Web-based backdoor malware is targeted at Web servers. When installed on a target system, remote users, even malicious users, may access this infected Web server using a browser such as Internet Explorer or Netscape Navigator. It compromises network security, and may be used to delete files and folders from infected systems.

PE_PERRUN.A (Aliases: W32.Perrun, W32/Perrun): This malware is a multi-component, non-destructive virus that attaches part of its code on JPEG files. This does not infect JPEG files and does NOT enable these files to propagate this malware. Affected JPEG files facilitate this malware's routine only on infected machines and behave as normal JPEG files on non-infected systems.

VBS/Chick-F (Alias: I-Worm.Brit-G) (Visual Basic Script Worm): This worm arrives as a compressed HTML file (CHM). When the file is opened, the worm displays the text "Enable activeX To See Korea Japan results." If the user enables the ActiveX script, the worm will search drives C:, D:, and E: looking for a mIRC installation. If the mIRC executable is located, the worm will copy itself into C:\<windows>\koreajapan.chm. VBS/Chick-F creates a mIRC script file script.ini in the mIRC directory. The script attempts to forward a copy of the worm to users that join the same IRC channel. Finally VBS/Chick-F sends an e-mail to the first entry in the user's Outlook address book. The e-mail will have the following characteristics:

- Subject line: RE: Korea Japan Results
- Message text: Take a look at these results ... Regards, <Current user>
- Attached file:<name of the worm file that is currently running>.

The following registry entry will be set to the value of "1" when the e-mailing routine has been executed:

- HKLM\Software\Microsoft\Windows\CurrentVersion\chm

This value acts as a marker and will prevent the e-mailing code from executing next time the worm is activated.

VBS/Gorum (Visual Basic Script Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book. If executed, the worm copies itself in the root directory (C:\) under the filenames XXXPic.exe." Additionally, any file it finds ending with the file extensions, *.bmp, *.doc, *.gif, *.htm, *.jpg, *.pdf, *.vbs, or *.xls, a second file will be created with the extension *.exe with the same file name. For example if "family_photos.gif" is found, the file "family_photos.exe" will be created.

VBS/VBSWG-AQ (Visual Basic Script Worm): This virus has been reported in the wild. It is an e-mail worm. The worm spreads using an e-mail with the following characteristics:

- Subject line: Shakira's Pics
- Message text: Hi : i have sent the photos via attachment have funn...
- Attached file: ShakiraPics.jpg.vbs

When the attachment is run, it will copy itself into the Windows folder and add the registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Registry

to ensure that the worm is run each time Windows is started. It will then attempt to e-mail itself to all addresses listed in the Microsoft Outlook address book. If the worm detects that mIRC is installed, it will create the file script.ini in the mIRC folder. VBS/VBSWG-AQ will also create the registry entries:

- HKCU\Software\ShakiraPics\mailed
- HKCU\Software\ShakiraPics\mirqued

after it has attempted to spread by e-mail and IRC. The worm will then search all local and network drives for files with VBE or VBS extensions and overwrite them with a copy of itself. Finally the worm will display the message "You have been infected by the ShakiraPics Worm."

VBS_NEMITE.A (Visual Basic Script Worm): This mass-mailing worm is a Visual Basic script (VBScript) that is embedded in an HTML (HyperText Markup Language) file. It propagates via e-mail, sending messages to all the recipients in an infected users address book. It modifies the Internet Explorer home page on the 3rd, 5th, and 28th day of the month, and sends out e-mail messages with the following characteristics:

- Subject: HI
- Message Body: KONO SYASHIN MITE NE !!!!
- Attachment: Syashin3.vbs

VBS_PETIK.G (Alias: PETIK.G, PETIK) (Visual Basic Script Worm): Upon execution, this mass-mailing worm drops a copy of itself in the root directory of drive C:\. It propagates using Microsoft Outlook or Outlook Express by sending itself to all entries listed in the infected user's address book.

VBS_PETIK.I (Alias: I-Worm.Petik.I) (Visual Basic Script Malware): This mass-mailing malware can disable the mouse and the keyboard of an infected computer. It propagates copies of itself as attachment in an e-mail with the following details:

- Subject: What is the seven sins ??
- Message Body: Look at this file and learn them.
- Attachment: Seven.vbs

VBS_TRILISSA.C (Aliases: TRILISSA.C, I-worm.trilissa.c) (Visual Basic Script Worm): The worm, WORM_TRILISSA.C, drops this mass-mailing malware. The worm uses this Visual Basic script malware to propagate copies of itself via e-mail to all addresses listed in infected users' Windows Address Books.

VBS_TRILISSA.D (Aliases: TRILISSA.D, I-worm.TRILISSA.D) (Visual Basic Script Worm): The worm, WORM_TRILISSA.D, drops this mass-mailing malware. It sends an e-mail with the following details to all recipients listed in the infected user's Windows Address Book:

- Subject: "Bush is a criminal!"
- Message Body: "Bush is a criminal!!!! See this screensaver!! HE IS A BASTARD!!!"
- Attachment: "Bush_you_are_guilty!!!.scr"

VBS.Slip@mm (Visual Basic Script Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all contacts in the Outlook Address Book

W32/Chir-A (Alias: I-Worm.Runouce) (Win32 Worm): This is an Internet worm that tries to spread via e-mail by sending itself to e-mail addresses found in the Windows address book. The e-mail will have the following characteristics:

- Sender address: <username>@hotmail.com or iloveyou@btamail.net.cn
- Subject line: Hi, i am <username>
- Attached file: p.exe

The worm attempts to exploit a MIME and an IFRAME vulnerability in some versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer to allow the executable file to run automatically without the user double clicking on the attachment. Microsoft has issued a patch that secures against this vulnerability which can be downloaded from Microsoft Security Bulletin MS01-027. (This patch was released to fix a number of vulnerabilities in Microsoft's software, including the one exploited by this worm.) When run, the worm copies itself into the Windows system folder as runouce.exe and sets the following registry entry so that the worm will be automatically started when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Runonce = C:\<Windows system folder>\runouce.exe

The worm also creates several EML files with the name <computername>.eml on network drives. These EML files contain a base64-encoded copy of the worm.

W32.Alcarys.G@mm (Aliases: WORM_NEYSID.A, W32.Neysid@mm, W97M.Alcarys.G@mm, W97M.Neysid@mm, X97M.Alcarys.G@mm, X97M.Neysid@mm) (Win32 Virus): This is a worm that is written in Visual Basic. It requires Visual Basic runtime libraries to function on a host system. It uses mIRC and Microsoft Outlook to spread, and it infects Microsoft Office documents and workbooks. The worm will arrive in an e-mail with 1 of 7 randomly chosen subjects, and 4 attachments (all copies of the worm). Three of the attachments are randomly named, and the 4th will be DISNEY.SCR. This worm attempts to distribute itself using files on systems that may be using the Kazaa file-sharing client application. When W32.Alcarys.G@mm is executed, it copies itself to several different locations on the hard disk and creates many copies of itself. It adds eight copies of itself on the desktop alone. Furthermore, it opens several Internet Explorer windows and it attempts to download an additional executable file.

W32.HLLW.Nople (Win32 Virus): This is a network-aware worm that copies itself to all remote computers as the file C:\Winnt\Noplease_flash_movie.exe. Indications that a computer has been infected are the presence of the Noplease_flash_movie.exe file or the message "Es hora de formatear tu disco."

W32.Pet_ticky.gen (Win32 Virus): This is a mass mailer that sends itself to all contacts in the Microsoft Outlook Address Book. The worm is a compiled Visual Basic executable that has been compressed with UPX. The worm arrives in an e-mail with the following characteristics:

- Subject: New Visual Tool for U
- Attachments: Visual_tool.exe

W32.Shermnar.Worm (Win32 Worm): This is a worm that attempts to spread through the peer-to-peer Kazaa network. It creates multiple copies of itself on an infected machine under a variety of names. It may be found as a file named NortonAntivirus2002UpdateInstaler.exe.

W97M.Locus (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and templates. This virus does not contain a damaging payload. W97M.Locus activates when opening infected documents. It checks for the presence of a high ASCII string in the macro module of host files. If the string is not found, the virus infects the host file. This virus has this comment line in the viral body:

- 'Locust_Ver.01

W97M.Nori.A (Word 97 Macro Virus): This is a Microsoft Word macro virus that carries a potentially very destructive payload. The payload is activated on April 1 of every year, and it deletes either all files on your hard disk (rare) or all the text from the body of infected documents. W97M.Nori.A spreads when an infected word document is opened or closed. It also spreads to any new document if that document is created while an infected document is active. During execution, W97M.Nori.A turns off the following settings in Word:

- Macro virus protection (VirusProtection)
- The prompt to confirm conversion when opening a document (ConfirmConversion)
- The prompt to confirm saving of the global template, Normal.dot (SaveNormalPrompt)

W97M.Nori.A also prevents you from viewing the Visual Basic Editor. During infection, W97M.Nori.A creates a temporary file named C:\Iron.tmp. It uses this file to spread between documents and the global template. After infection, the virus deletes this file.

WORM_CHIR.A (Aliases: W32/Chir@MM, I-Worm.Runouce, Win32/Chir.A@mm) (Internet Worm): This worm propagates by sending the following e-mail to all addresses in an infected user's Microsoft Outlook address book:

- From: iloveyou@btamail.net.cn
- Message Body:
- Subject: Hi, i am &ltusername>
- Attachment: P.exe

WORM_ENEMANY.D (Aliases: W32.Enemany.D@mm, ENEMANY.D) (Internet Worm): This nondestructive, non-memory resident mass-mailing worm sends copies of itself via e-mail to all contacts listed in an infected user's Microsoft Outlook address book.

WORM_FISHLET.A (Internet Worm): This mass-mailing worm uses its own SMTP (Simple Mail Transfer Protocol) engine to send copies of itself to all e-mail addresses that it finds in the Microsoft (WAB) Windows Address Book. The e-mail messages arrive with the following characteristics:

- Subject: Order
- Message Body: Dear eBay customer,
  Thank you for using eBay Services.

  _____
  Your order Num. is: 31547
  Delivery time: 7 days ...
- Attachment: ???.exe

*where ??? is a random filename

WORM_FRETHEM.B (Internet Worm): This memory-resident variant of WORM_FRETHEM.A propagates via e-mail, using its own SMTP engine to send e-mail messages with the subject line "Re: Your password!" It gathers e-mail addresses from the infected user's Windows Address Book (WAB) and from certain files in Microsoft Outlook Express mail archives.

WORM_FRETHEM.C (Alias: I-Worm.Frethem.c) (Internet Worm): This memory-resident variant of WORM_FRETHEM.A propagates via e-mail, using its own SMTP (Simple Mail Transfer Protocol) engine to send e-mail messages with itself as an attachment. It gathers e-mail addresses from an infected user's Windows Address Book (WAB) and from certain files in Microsoft Outlook Express mail archives. This worm sends out e-mail messages with the following details:

- Subject: Re: Your password!
- Message Body: Your password is W8dqwq8q918213
- Attachment: Your password placed in password.txt yourpassword.exe

WORM_FRETHEM.D (Alias: W32.Frethem.D@mm) Win32 Worm): This nondestructive variant of WORM_FRETHEM.A, a memory-resident worm, propagates as an attachment in an e-mail with the following details:

- Subject: Re: Your password!
- Message Body: ATTENTION! You can access very important information by this password DO NOT SAVE password to disk use your mind now press cancel
- Attachment: Decrypt-password.exe

This worm sends the e-mail to all e-mail addresses listed in the infected user's Windows Address Book and in .DBX files, in which the Microsoft Outlook Express archives e-mails.

WORM_FRETHEM.E (Aliases: W32.Frethem.D@mm, FRETHEM.E) (Internet Worm): This non-destructive, memory-resident variant of WORM_FRETHEM.A propagates via Microsoft Outlook by sending e-mail to all addresses listed in the infected user's Windows Address Book, and in .DBX files where Microsoft Outlook Express archives e-mails. It arrives as an attachment to an e-mail message with the following:

- Subject: Re: Your password!
- Message Body: ATTENTION! You can access very important information by this password DO NOT SAVE password to disk use your mind now press cancel
- Attachments: Decrypt-password.exe password.txt

The file attachment, DECRYPT-PASSWORD.EXE, automatically executes when this e-mail message is previewed or opened.

WORM_FRETHEM.F (Internet Worm): This variant of WORM_FRETHEM.B propagates via e-mail, using its own SMTP (Simple Mail Transfer Protocol) engine to send e-mail messages with a copy of itself as an attachment. It gathers e-mail addresses from the infected user's Windows Address Book (WAB) and

from certain files in Microsoft Outlook Express mail archives. This worm sends out e-mail messages with the following characteristics:

- Subject: Re: Your password!
- Message Body: Your password is W8dqwq8q918213
- Attachment: Your password placed in password.txt yourpassword.exe

WORM_PETLIL.A (Aliases: W32.Pet_Ticky.B@mm, W32/PetLil@MM, Win32.Petlil.A) (Internet Worm): This non-destructive, mass-mailing worm propagates via e-mail using Microsoft Outlook. Upon execution, it displays a message box. On the 1st, 15th, and 31st day of each month, it displays a picture of a semi-nude woman instead.

WORM_TRILISSA.C (Aliases: TRILISSA.C, I-Worm.Trilissa.c) (Internet Worm): This mass-mailing worm is dependent on a dropped Visual Basic script file, VBS_TRILISSA.C, for its propagation. Once this worm has been executed, it displays a series of messages. This worm arrives as an attachment in e-mail messages with the following details:

- Subject: "Mira el salvapantallas de Shakira!"
- Message Body: "Shakira!! Mejor que la farlopa!! Miralo!!"
- Attachment: "Shakira.scr"

WORM_TRILISSA.D (Aliases: TRILISSA.D, I-Worm.TRILISSA.D) (Internet Worm): This mass-mailing worm uses another malware, VBS_TRILISSA.D, to propagate copies of itself. Upon execution, it displays a series of messages. This worm arrives as an attachment in e-mail messages with the following characteristics:

- Subject: "Bush is a criminal!"
- Message Body: "Bush is a criminal!!!! See this screensaver!! HE IS A BASTARD!!!"
- Attachment: "Bush_you_are_guilty!!!.scr"

WORM_WORTRON.10B (Alias: wortron.10b) (Internet Worm): The Trojan, TROJ_WORTRON.10B generates this worm, which propagates via e-mail. It sends copies of itself to all e-mail recipients listed in the infected user's Windows Address Book.

WPRO_SPENTY.A (Alias: WordPro.Spenty) (Macro Virus): This virus has been reported in the wild. It is a destructive Lotus Word Pro Macro file infector that infects files as they are opened or created. It replicates only in Chinese versions of Word Pro. The security settings of infected documents are changed to allow editing only by the creator of the document, and only when the correct password is entered. The password is "720401." In Chinese versions of Word Pro, several menus, including the Scripts menu, do not function correctly while the virus is running. If the virus is executed during May or on the 20th of any month, then the virus attempts to download a file from several Web sites. If it succeeds, then the file is displayed and the Autoexec.bat file is altered to contain instructions to delete the contents of drives C, D, and E.

X97M/Anis (Alias: Bdoc2) (Excel 97 Macro Virus): When an infected workbook is opened, X97M/Anis.A creates "AutoRun.xla" into Excel's startup directory and infects it. The virus infects all workbooks that are opened, closed or saved. It attempts to disable items from the "Tools" menu and attempts to hook items in the "File" menu. Anis has two different payloads. When saving a workbook or exiting the program, it checks if the current day is 5th, 10th, 15th, 20th, 25th, or 30th, and if so, it shuts down Windows. The virus also displays a message on 26th of every month, written in Japanese. Therefore the message is not readable on versions of Excel that do not support doublebyte characters, such as the English version.

XM97/Pathetic-D (Alias: XM97/Pathe-D) (Excel 97 Macro Virus): This virus has been reported in the wild. It is an Excel 97 macro virus that replicates using a file called Book1.xls in the XLSTART folder. The virus appends the text "@echo T'as été mordu par... Le bec du Saumon " to C:\autoexec.bat and on any day in May it will close the active workbook.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2002-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
APStrojan.sl	N/A	CyberNotes-2002-03
Arial	N/A	CyberNotes-2002-08
Backdoor.AntiLam	**N/A**	**Current Issue**
Backdoor.Crat	**N/A**	**Current Issue**
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.FTP_Bmail	**N/A**	**Current Issue**
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.GSpot	**N/A**	**Current Issue**
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.Latinus	**N/A**	**Current Issue**
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Nota	**N/A**	**Current Issue**
Backdoor.Omed.B	N/A	CyberNotes-2002-11
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Systsec	N/A	CyberNotes-2002-04
Backdoor.Tron	**N/A**	**Current Issue**
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
BDS/ConLoader	**N/A**	**Current Issue**
BDS/Osiris:	N/A	CyberNotes-2002-06
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
BKDR_SMALLFEG.A	N/A	CyberNotes-2002-04
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
Dewin	N/A	CyberNotes-2002-08
DlDer	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Downloader-W	N/A	CyberNotes-2002-08
Fortnight	N/A	CyberNotes-2002-10

Trojan	Version	CyberNotes Issue #
Hacktool.IPStealer	N/A	CyberNotes-2002-02
Irc-Smallfeg	N/A	CyberNotes-2002-03
IRC-Smev	N/A	CyberNotes-2002-08
JS/NoClose	N/A	CyberNotes-2002-11
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11
RCServ	N/A	CyberNotes-2002-10
SecHole.Trojan	N/A	CyberNotes-2002-01
TR/Win32.Rewin	**N/A**	**Current Issue**
Tr/WiNet	N/A	CyberNotes-2002-10
TR/Zirko	N/A	CyberNotes-2002-10
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/DSS-A	**N/A**	**Current Issue**
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DSNX.A	N/A	CyberNotes-2002-03
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_WORTRON.10B	**N/A**	**Current Issue**
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.CrazyBilets	**N/A**	**Current Issue**
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS.Gascript	N/A	CyberNotes-2002-04
VBS_CHICK.B	N/A	CyberNotes-2002-07

Trojan	Version	CyberNotes Issue #
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Libi	N/A	CyberNotes-2002-10
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Tendoolf	N/A	CyberNotes-2002-09
WbeCheck	N/A	CyberNotes-2002-09

Backdoor.AntiLam: This s a typical backdoor Trojan, which gives a remote malicious user unobstructed access to your computer. When Backdoor.AntiLam is run, it does the following:

- It copies itself into the %Windows% folder. The exact file names that are used by the Trojan may vary from version to version, because the malicious user who creates this backdoor Trojan can choose any desired file name. By default, the file name is Scandisk.exe (NOTE: %Windows% is a variable. The worm locates the \Windows folder (by default this is C:\Windows or C:\Winnt) and copies itself into that location.)
- It adds the value: MS Scandisk <dropped file such as Scandisk.exe> to the registry key:
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- It also adds the value: Start ok to the registry key:
  - HKEY_LOCAL_MACHINE\Software\Microsoft\DirectX

The Trojan then opens an HTTP connection to a Web server that the malicious user chooses, and posts victim information to a script at that Web site. If Backdoor.AntiLam is run, it allows the malicious user to remotely take control over the compromised computer, and can include:

- Repeatedly open a TCP port
- Display a fake error message to conceal its true nature
- Full control over the file system
- Upload to and download from the host computer
- Run files of the hacker's choice
- Display messages
- View the screen
- Log keystrokes
- Annoying actions, such as manipulate the keyboard or mouse, open and close the CD-ROM drive, turn the monitor on and off, and so on.

Backdoor.Crat: Backdoor.Crat allows a malicious user to remotely control an infected computer. It is written in the Delphi program language and compressed with Ezip. When Backdoor.Crat runs, it copies itself to the %System% folder. The exact file names and port numbers that it uses may vary from version to version, because the malicious user who creates this Backdoor Trojan can choose any desired file name. For example, the file name can be Winload.exe. It adds the value:

- WinDLL C:\%System%\<dropped file name>

to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Backdoor.FTP_Bmail (Aliases: Backdoor.FTP.Bmail, BackDoor-ABH): This is a Trojan horse that allows a malicious user to remotely control an infected computer. It disguises itself as an FTP downloader for e-mail software. When you run Backdoor.FTP_Bmail, it tries to connect to a FTP server. The Trojan contains the following string in its code:

- "Would you like to download Bmail.. Bmail is a talking E-mail software that works with POP and other e-mail accounts. Its works with Yahoo and Onebox also. More will be added soon.."

Besides opening the FTP connection, the Trojan opens TCP port 5135 and a randomly changed TCP/UDP port. This gives a remote attacker access to the compromised computer. The Trojan adds a value:

- setFTPBack C:\%system%\createsw.exe

to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Backdoor.GSpot (Alias: Trojan.W32.G-Spot): This is a Trojan horse which allows unauthorized access to an infected computer by using the GSpot client program. It is the server portion of the GSpot client. If it is installed, it drops the file \Windows\System\Msregdrv32.exe. It adds the value, "Video Driver," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run

When installed, the Trojan displays the file \Windows\Temp\Temp2.jpg. This file is not malicious and can be deleted. It also drops the file \Windows\Temp\Temp1.exe, which is identical to Msregdev32.exe, and should also be deleted. This Delphi code uses sockets to look for open ICQ connections and possible hosts.

Backdoor.Latinus (Alias: Backdoor.Trojan): Backdoor.Latinus allows a malicious user to remotely control an infected computer. There are numerous versions of this Trojan.

Backdoor.Nota: This is a typical Backdoor Trojan that allows a malicious user to gain access to and remotely control an infected computer. The Trojan program is written in the Delphi programming language and compressed with UPX. When Backdoor.Nota runs, it copies itself as:

- C:\%System%\ActiveDesktop.exe
- C:\%Windows%\Mdm.exe
- C:\%Windows%\winfat32.exe
- C:\%Windows%\All Users\Start Menu\Programs\StartUp\Explorer.exe

It modifies the following system files:

- C:\Windows\Win.ini. It adds the following lines to the [Windows] section:
  load=run=SYSTEM\ActiveDesktop.exe
  NullPort=None
- C:\Windows\System.ini. It adds the following line:
  shell=Explorer.exe winfat32.exe

These changes cause the Trojan to be executed automatically when you start Windows. The Trojan opens numerous TCP ports, including 61337 and other randomly chosen ports, to give the remote malicious user unobstructed access to the compromised computer. The Trojan may drop the following files:

- C:\%Windows%\Scpt.sys
- C:\%Windows%\Temp254.ini

The Trojan uses these files to store stolen information.

Backdoor.Tron: This is a backdoor Trojan that allows unauthorized access to an infected system. This backdoor attempts to kill the processes of several versions of the ZoneAlarm firewall and Tiny Personal Firewall (version 2.0.15.0); this allows Backdoor.Tron to gain access to the system without being detected by those firewalls.

BDS/ConLoader: This is a backdoor server program. It will potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan adds the following file to the \windows\ directory, "@ye." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
  "Configuration Loader"="@ýe"

TR/Win32.Rewin: Like other Trojans, TR/Win32.Rewin would potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan adds the following file to the \windows\ directory, "winrep.com." Additionally, the file "Dialer.com" also gets created in the \windows\%system% directory. So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
  "Win32RG"="c:\\windows\\Winrep.com"
  "Win32GR"="c:\\windows\\system\\Dialer.com"

Troj/DSS-A: This is a Trojan that drops the file, INDEX.HTM, into the Windows Temp folder. The Trojan then opens this file in a hidden browser window. INDEX.HTM contains an HTML script which attempts to connect to a web site about twenty minutes after opening. The web site contains an advertisement for a web site with pornographic content and may attempt to drop a dialler program onto the user's computer. The behavior of Troj/DSS-A may be altered dynamically by changing the contents of the web page to which it connects. The Trojan file is likely to arrive in an e-mail as an attachment called OPENME.EXE.

TROJ_WORTRON.10B (Alias: Trojan.PSW.Wortron.10.b): This Trojan and Worm Generator can run on any Windows platform. On its own, it does not have a destructive payload or routine. However, its generated Trojans and worms may be destructive, depending on the configurations that the malicious user using this Trojan, does on the generated malware.

Trojan.PSW.CrazyBilets: This program belongs to the family of passwords stealing Trojans. On June 2, a site with the descriptive name Graduates of 2002, was exposed operating in the public access home pages of Narod.ru. The anonymous author offered visitors the chance to download a file containing the actual exams for literature and mathematics. When the file is downloaded, what actually happens is the file copies a list with essays, allegedly the compositions sought by the students and of course with it came the Trojan program named CrazyBilets. The web page contained the following:

- Intermediate Examinations
- Test papers for mathematics and topics for compositions. Still FREE!

The file residing on the web page is a Trojan installer. When run, it drops a Trojan program into the Windows directory, then extracts and creates fake examination topics (in Russian). The Trojan itself is a Windows PE EXE file about 27Kb in length (compressed by UPX, the decompressed size is about 83Kb) and written in Delphi. When executed, the Trojan copies itself to the Windows directory under the SYSTEM.EX name and registers this file in system registry auto-run key:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run System = %WindowsDir%\System.exe

The main function for the CrazyBilets Trojan are collecting cached Windows passwords on victim machines and sending this information to its "master" by direct connection to an SMTP server.